

ABSTRACT

The present invention provides an online transaction method for providing a user with an online transaction via a digital media in an online transaction system. The online transaction system comprises a certificate authority module, at least one service provider module, at least one management module and a transaction module. Each management module respectively has an authentication device and a transaction device. The authentication device is connected between the service provider module and the certificate authority module. The transaction device is connected between the service provider module and the transaction module.

The online transaction method comprises the following steps of registering a digital certificate in the certificate authority module by the user via the digital media for generating a log data, the certificate authority module outputting the log data to the authentication device of the management module in a predetermined period; inputting the digital certificate in the service provider module by the user via the digital media for generating a digital signature, the service provider module outputting the digital signature to the authentication device of the management module; authenticating the digital signature according to a predetermined procedure for generating an authentication code; verifying the effectiveness of the user's authentication in the service provider module, and providing the user with the online transaction for generating a corresponding first transaction data to the transaction module; processing the first transaction data in the transaction module for generating a second transaction data to the transaction device of the management module; recording the second transaction data in the transaction device, and outputting the second transaction data to the service provider module; and displaying the second transaction data in the service provider module. In the online transaction system of the present invention, the digital signature, the authentication code, the first transaction data and the second transaction data are respectively based on the digital certificate for encryption in the transmission process. Therefore, the security problems of online transactions can be greatly improved.